

$H(X)$ vs. $H(f(X))$

Ferdinando Cicalese
Università di Verona, Verona, Italy
Email: cclfdn22@univr.it

Luisa Gargano
Università di Salerno, Salerno, Italy
Email: lgargano@unisa.it

Ugo Vaccaro
Università di Salerno, Salerno, Italy
Email: uvaccaro@unisa.it

Abstract—It is well known that the entropy $H(X)$ of a finite random variable is always greater or equal to the entropy $H(f(X))$ of a function f of X , with equality if and only if f is one-to-one. In this paper, we give tight bounds on $H(f(X))$ when the function f is not one-to-one, and we illustrate a few scenarios where this matters. As an intermediate step towards our main result, we prove a lower bound on the entropy of a probability distribution, when only a bound on the ratio between the maximum and the minimum probability is known. Our lower bound improves previous results in the literature, and it could find applications outside the present scenario.

I. THE PROBLEM

Let $\mathcal{X} = \{x_1, \dots, x_n\}$ be a finite alphabet, and X be any random variable (r.v.) taking values in \mathcal{X} according to the probability distribution $\mathbf{p} = (p_1, p_2, \dots, p_n)$, that is, such that $P\{X = x_i\} = p_i$, for $i = 1, 2, \dots, n$. A well known and widely used inequality (see [5], Exercise 2.4), states that

$$H(f(X)) \leq H(X), \quad (1)$$

where $f : \mathcal{X} \rightarrow \mathcal{Y}$ is any function defined on \mathcal{X} , and $H(\cdot)$ denotes the Shannon entropy. Moreover, equality holds in (1) if and only if f is one-to-one. The main purpose of this paper is to sharpen inequality (1) by deriving tight bounds on $H(f(X))$ when f is not one-to-one. More precisely, given the r.v. X , an integer $2 \leq m < n$, a set $\mathcal{Y}_m = \{y_1, \dots, y_m\}$, and the family of surjective functions $\mathcal{F}_m = \{f : \mathcal{X} \rightarrow \mathcal{Y}_m, |f(\mathcal{X})| = m\}$, we want to compute the values

$$\max_{f \in \mathcal{F}_m} H(f(X)) \quad \text{and} \quad \min_{f \in \mathcal{F}_m} H(f(X)). \quad (2)$$

II. THE RESULTS

For any probability distribution $\mathbf{p} = (p_1, p_2, \dots, p_n)$, with $p_1 \geq p_2 \geq \dots \geq p_n \geq 0$, and integer $2 \leq m < n$, let us define the probability distributions $R_m(\mathbf{p}) = (r_1, \dots, r_m)$ as follows: if $p_1 < 1/m$ we set $R_m(\mathbf{p}) = (1/m, \dots, 1/m)$, whereas if $p_1 \geq 1/m$ we set $R_m(\mathbf{p}) = (r_1, \dots, r_m)$, where

$$r_i = \begin{cases} p_i & \text{for } i = 1, \dots, i^* \\ \left(\sum_{j=i^*+1}^n p_j \right) / (m - i^*) & \text{for } i = i^* + 1, \dots, m, \end{cases} \quad (3)$$

and i^* is the maximum index i such that $p_i \geq \frac{\sum_{j=i+1}^n p_j}{m-i}$. A somewhat similar operator was introduced in [9].

Additionally, we define the probability distributions $Q_m(\mathbf{p}) = (q_1, \dots, q_m)$ in the following way:

$$q_i = \begin{cases} \sum_{k=1}^{n-m+1} p_k, & \text{for } i = 1, \\ p_{n-m+i}, & \text{for } i = 2, \dots, m. \end{cases} \quad (4)$$

The following Theorem provides the results sought in (2).

Theorem 1. *For any r.v. X taking values in the alphabet $\mathcal{X} = \{x_1, x_2, \dots, x_n\}$ according to the probability distribution $\mathbf{p} = (p_1, p_2, \dots, p_n)$, and for any $2 \leq m < n$, it holds that*

$$\max_{f \in \mathcal{F}_m} H(f(X)) \in [H(R_m(\mathbf{p})) - \alpha, H(R_m(\mathbf{p}))], \quad (5)$$

where $\alpha = 1 - (1 + \ln(\ln 2)) / \ln 2 < 0.0861$, and

$$\min_{f \in \mathcal{F}_m} H(f(X)) = H(Q_m(\mathbf{p})). \quad (6)$$

Therefore, the function $f \in \mathcal{F}_m$ for which $H(f(X))$ is minimum maps all the elements $x_1, \dots, x_{n-m+1} \in \mathcal{X}$ to a single element, and it is one-to-one on the remaining elements x_{n-m+2}, \dots, x_n .

Before proving Theorem 1 and discuss its consequences, we would like to notice that there are quite compelling reasons why we are unable to determine the exact value of the maximum in (5), and consequently, the form of the function $f \in \mathcal{F}_m$ that attains the bound. Indeed, computing the value $\max_{f \in \mathcal{F}_m} H(f(X))$ is an NP-hard problem. It is easy to understand the difficulty of the problem already in the simple case $m = 2$. To that purpose, consider any function $f \in \mathcal{F}_2$, that is $f : \mathcal{X} \rightarrow \mathcal{Y}_2 = \{y_1, y_2\}$, and let X be any r.v. taking values in \mathcal{X} according to the probability distribution $\mathbf{p} = (p_1, p_2, \dots, p_n)$. Let $z_1 = \sum_{x \in \mathcal{X} : f(x) = y_1} P\{X = x\}$, $z_2 = \sum_{x \in \mathcal{X} : f(x) = y_2} P\{X = x\}$. Then, $H(f(X)) = -z_1 \log z_1 - z_2 \log z_2$, and it is maximal in correspondence of a function $f \in \mathcal{F}_2$ that makes the sums z_1 and z_2 as much equal as possible. This is equivalent to the well known NP-hard problem PARTITION on the instance $\{p_1, \dots, p_n\}$ (see [7])². Since the function $f \in \mathcal{F}_m$ for which $H(f(X)) \geq H(R_m(\mathbf{p})) - \alpha$ can be efficiently constructed, we have also the following important consequence of Theorem 1.

Corollary 1. *There is a polynomial time algorithm to approximate the NP-hard problem of computing the value*

$$\max_{f \in \mathcal{F}_m} H(f(X)),$$

with an additive approximation factor of $\alpha \leq 0.0861$.

¹Here, with a slight abuse of notation, for a probability distribution $\mathbf{a} = (a_1, \dots, a_t)$ we denote with $H(\mathbf{a}) = -\sum_i a_i \log a_i$ the entropy of a discrete r.v. distributed according to \mathbf{a} . Moreover, with \log we denote the logarithm in base 2, and with \ln the natural logarithm in base e .

²In the full version of the paper we will show that the problem of computing the value $\max_{f \in \mathcal{F}_m} H(f(X))$ is strongly NP-hard.

A key tool for the proof of Theorem 1 is the following result, proved in the second part of Section IV.

Theorem 2. *Let $\mathbf{p} = (p_1, p_2, \dots, p_n)$ be a probability distribution such that $p_1 \geq p_2 \geq \dots \geq p_n > 0$. If $p_1/p_n \leq \rho$ then*

$$H(\mathbf{p}) \geq \log n - \left(\frac{\rho \ln \rho}{\rho - 1} - 1 - \ln \frac{\rho \ln \rho}{\rho - 1} \right) \frac{1}{\ln 2}. \quad (7)$$

Theorem 2 improves on several papers (see [17] and references therein quoted), that have studied the problem of estimating $H(\mathbf{p})$ when only a bound on the ratio p_1/p_n is known.³ We believe the result to be of independent interest. For instance, it can also be used to improve existing bounds on the leaf-entropy of parse trees generated by Tunstall algorithm.

To prove our results, we use ideas and techniques from Majorization Theory [15], a mathematical framework that has been proved to be very much useful in Information Theory (e.g., see [2], [3], [9], [10] and references therein quoted).

III. SOME APPLICATIONS

Besides its inherent naturalness, the problem of estimating the entropy $H(f(X))$ vs. $H(X)$ has several interesting applications. We highlight some of them here, postponing a more complete discussion in the full version of the paper.

In the area of clustering, one seeks a mapping f (deterministic or stochastic) from some data, generated by a r.v. X taking values in a set \mathcal{X} , to “clusters” in \mathcal{Y} , where $|\mathcal{Y}| \ll |\mathcal{X}|$. A widely employed measure to appraise the goodness of a clustering algorithm is the information that the clusters retain towards the original data, measured by the mutual information $I(X; f(X))$ (see [6], [11] and references therein quoted). In general, one wants to choose f such that $|f(\mathcal{X})|$ is small but $I(X; f(X))$ is large. The authors of [8] (see also [13]) proved that, given the random variable X , among all mappings f that maximizes $I(X; f(X))$ (under the constraint that $|f(\mathcal{X})|$ is fixed) there is a maximizing function f that is *deterministic*. Since in the case of deterministic functions it holds that $I(X; f(X)) = H(f(X))$, finding the clustering f of \mathcal{X} (into a fixed number m of clusters) that maximizes the mutual information $I(X; f(X))$ is *equivalent* to our problem of finding the function f that attains the upper bound in (2).⁴

Another scenario where our results directly find applications is the one considered in [18]. There, the author considers the problem of best approximating a probability distribution $\mathbf{p} = (p_1, \dots, p_n)$ with a shorter one $\mathbf{q}^* = (q_1^*, \dots, q_m^*)$, $m \leq n$. The criterion with which one chooses \mathbf{q}^* , given \mathbf{p} , is the following. Given $\mathbf{p} = (p_1, \dots, p_n)$ and $\mathbf{q} = (q_1, \dots, q_m)$,

define the quantity $D(\mathbf{p}, \mathbf{q})$ as $2W(\mathbf{p}, \mathbf{q}) - H(\mathbf{p}) - H(\mathbf{q})$, where $W(\mathbf{p}, \mathbf{q})$ is the *minimum* entropy of a bivariate probability distribution that has \mathbf{p} and \mathbf{q} as marginals. Then, the “best” approximation \mathbf{q}^* of \mathbf{p} is chosen as the probability distributions \mathbf{q}^* with m components that *minimizes* $D(\mathbf{p}, \mathbf{q})$, over all $\mathbf{q} = (q_1, \dots, q_m)$. The author of [18] shows that \mathbf{q}^* can be characterized in the following way. Given $\mathbf{p} = (p_1, \dots, p_n)$, call $\mathbf{q} = (q_1, \dots, q_m)$ an *aggregation* of \mathbf{p} into m components if there is a partition of $\{1, \dots, n\}$ into disjoint sets I_1, \dots, I_m such that $q_k = \sum_{i \in I_k} p_i$, for $k = 1, \dots, m$. In [18] it is proved that the vector \mathbf{q}^* that best approximate \mathbf{p} (according to D) is the aggregation of \mathbf{p} into m components of *maximum entropy*. Since *any* aggregation \mathbf{q} of \mathbf{p} can be seen as the distribution of the r.v. $f(X)$, where f is some appropriate function and X is a r.v. distributed according to \mathbf{p} (and, vice versa, any deterministic f gives a r.v. $f(X)$ whose distribution is an aggregation of the distribution of X), one gets that the problem of computing the “best” approximation \mathbf{q}^* of \mathbf{p} is NP-hard. The bound (5) allows us to provide an approximation algorithm to construct a probability distribution $\bar{\mathbf{q}} = (\bar{q}_1, \dots, \bar{q}_m)$ such that $D(\mathbf{p}, \bar{\mathbf{q}}) \leq D(\mathbf{p}, \mathbf{q}^*) + 0.0861$, improving on [4], where an approximation algorithm for the same problem with an additive error of 1 was provided.

There are other problems that can be cast in our scenario. For instance, Baez *et al.* [1] give an axiomatic characterization of the Shannon entropy in terms of *information loss*. Stripping away the Category Theory language of [1], the information loss of a r.v. X amounts to the difference $H(X) - H(f(X))$, where f is any deterministic function. Our Theorem 1 allows to quantify the extreme value of the information loss of a r.v., when the support of $f(X)$ is known.

There is also a vast literature (see [14], Section 3.3, and references therein quoted) studying the “*leakage of a program* P [...] defined as the (Shannon) entropy of the partition $\Pi(P)$ ” [14]. One can easily see that their “leakage” is the same as the entropy $H(f(X))$, where X is the r.v. modeling the program input, and f is the function describing the input-output relation of the program P . In Section 8 of the same paper the authors study the problem of maximizing or minimizing the leakage, in the case the program P is stochastic, using standard techniques based on Lagrange multipliers. They do not consider the (harder) case of deterministic programs (i.e., deterministic f ’s) and our results are likely to be relevant in that context.

Finally, we remark that our problem can also be seen as a problem of quantizing the alphabet of a discrete source into a smaller one (e.g., [16]), and the goal is to maximize the mutual information between the original source and the quantized one.

³The bound in [17] has this form: if $p_1/p_n \leq 1 + 2(e^\epsilon - 1) + 2\sqrt{e^{2\epsilon} - e^\epsilon}$, then $H(X) \geq \log n - \epsilon$. One can see that our bound (7) is tighter.

⁴In [13] the authors consider the problem of determining the function f that maximizes $I(X; f(Y))$, where X is the r.v. at the input of a DMC and Y is the corresponding output. Our scenario could be seen as the particular case when the DMC is noiseless. However, the results in [13] do not imply ours since the authors give algorithms only for binary input channels (i.e. $n = 2$, that makes the problem completely trivial in our case). Instead, our results are relevant to those of [13]. For instance, we obtain that the general maximization problem considered in [13] is NP-hard, a fact unnoticed in [13].

IV. THE PROOFS

We first recall the important concept of *majorization* among probability distributions.

Definition 1. [15] *Given two probability distributions $\mathbf{a} = (a_1, \dots, a_n)$ and $\mathbf{b} = (b_1, \dots, b_n)$ with $a_1 \geq \dots \geq a_n \geq 0$*

and $b_1 \geq \dots \geq b_n \geq 0$, we say that \mathbf{a} is majorized by \mathbf{b} , and write $\mathbf{a} \preceq \mathbf{b}$, if and only if

$$\sum_{k=1}^i a_k \leq \sum_{k=1}^i b_k, \quad \text{for all } i = 1, \dots, n.$$

Without loss of generality we assume that *all* the probabilities distributions we deal with have been ordered in non-increasing order. We also use the majorization relationship between vectors of unequal lengths, by properly padding the shorter one with the appropriate number of 0's at the end.

Consider an arbitrary function $f : \mathcal{X} \rightarrow \mathcal{Y}$, $f \in \mathcal{F}_m$. Any r.v. X taking values in $\mathcal{X} = \{x_1, \dots, x_n\}$, according to the probability distribution $\mathbf{p} = (p_1, \dots, p_n)$, and the function f naturally induce a r.v. $f(X)$, taking values in $\mathcal{Y} = \{y_1, \dots, y_m\}$ according to the probability distribution whose values are given by the expressions

$$\forall y_j \in \mathcal{Y} \quad P\{f(X) = y_j\} = \sum_{x \in \mathcal{X}: f(x)=y_j} P\{X = x\}. \quad (8)$$

Let $\mathbf{z} = (z_1, \dots, z_m)$ be the vector containing the values $z_1 = P\{f(X) = y_1\}, \dots, z_m = P\{f(X) = y_m\}$ ordered in non-increasing fashion. For convenience, we state the following self-evident fact about the relationships between \mathbf{z} and \mathbf{p} .

Claim 1. *There is a partition of $\{1, \dots, n\}$ into disjoint sets I_1, \dots, I_m such that $z_j = \sum_{i \in I_j} p_i$, for $j = 1, \dots, m$.*

Therefore, \mathbf{z} is an aggregation of \mathbf{p} . Given a r.v. X distributed according to \mathbf{p} , and any $f \in \mathcal{F}_m$, by simply applying the definition of majorization one can see that the (ordered) probability distribution of the r.v. $f(X)$ is majorized by $Q_m(\mathbf{p}) = (q_1, \dots, q_m)$, as defined in (4). Therefore, by invoking the Schur concavity of the entropy function H (see [15], p. 101 for the statement, and [10] for an improvement), saying that $H(\mathbf{a}) \geq H(\mathbf{b})$ whenever $\mathbf{a} \preceq \mathbf{b}$, we get that $H(f(X)) \geq H(Q_m(\mathbf{p}))$. From this, the equality (6) immediately follows.

We need the following two simple results, but important to us, stated and proved in [4] with a different terminology.

Lemma 1. [4] *For \mathbf{p} and \mathbf{z} as above, it holds that $\mathbf{p} \preceq \mathbf{z}$.*

In other words, for any r.v. X and function f , the probability distribution of $f(X)$ always majorizes that of X .

Lemma 2. [4] *For any m , $2 \leq m < n$, and probability distribution $\mathbf{a} = (a_1, \dots, a_m)$ such that $\mathbf{p} \preceq \mathbf{a}$, it holds that*

$$R_m(\mathbf{p}) \preceq \mathbf{a}, \quad (9)$$

where $R_m(\mathbf{p})$ is the probability distribution defined in (3).

From Lemmas 1 and 2, and by applying the Schur concavity of the entropy function H , we get the following result.

Corollary 2. *For any r.v. X taking values in \mathcal{X} according to a probability distribution \mathbf{p} , and for any $f \in \mathcal{F}_m$, it holds that*

$$H(f(X)) \leq H(R_m(\mathbf{p})). \quad (10)$$

Above corollary implies that

$$\max_{f \in \mathcal{F}_m} H(f(X)) \leq H(R_m(\mathbf{p})).$$

Therefore, to complete the proof of Theorem 1 we need to show that we can construct a function $f \in \mathcal{F}_m$ such that

$$H(f(X)) \geq H(R_m(\mathbf{p})) - \left(1 - \frac{1 + \ln(\ln 2)}{\ln 2}\right), \quad (11)$$

or, equivalently, that we can construct an aggregation of \mathbf{p} into m components, whose entropy is at least $H(R_m(\mathbf{p})) - \left(1 - \frac{1 + \ln(\ln 2)}{\ln 2}\right)$. We prove this fact in the following lemma.

Lemma 3. *For any $\mathbf{p} = (p_1, \dots, p_n)$ and $2 \leq m < n$, we can construct an aggregation $\mathbf{q} = (q_1, \dots, q_m)$ of \mathbf{p} such that*

$$H(\mathbf{q}) \geq H(R_m(\mathbf{p})) - \left(1 - \frac{1 + \ln(\ln 2)}{\ln 2}\right).$$

Proof: We will assemble the aggregation \mathbf{q} through the Huffman algorithm. We first make the following observation. To the purposes of this paper, each *step* of the Huffman algorithm consists in merging the two smallest element x and y of the current probability distribution, deleting x and y and substituting them with the single element $x+y$, and *reordering* the new probability distribution from the largest element to the smallest (ties are arbitrarily broken). Immediately after the step in which x and y are merged, *each* element z in the new and reduced probability distribution that finds itself positioned at the “right” of $x+y$ (if there is such a z) has a value that satisfies $(x+y) \leq 2z$ (since, by choice, $x, y \leq z$). Let $\mathbf{q} = (q_1, \dots, q_m)$ be the ordered probability distribution obtained by executing *exactly* $n-m$ steps of the Huffman algorithm, starting from the distribution \mathbf{p} . Denote by i_q the maximum index i such that for each $j = 1, \dots, i_q$ the component q_j has not been produced by a merge operation of the Huffman algorithm. In other word, i_q is the maximum index i such that for each $j = 1, \dots, i_q$ it holds that $q_j = p_j$. Notice that we allow i_q to be equal to 0. Therefore q_{i_q+1} has been produced by a merge operation. At the step in which the value q_{i_q+1} was created, it holds that $q_{i_q+1} \leq 2z$, for any z at the “right” of q_{i_q+1} . At later steps, the inequality $q_{i_q+1} \leq 2z$ still holds, since elements at the right of q_{i_q+1} could have only increased their values.

Let $S = \sum_{k=i_q+1}^m q_k$ be the sum of the last (smallest) $m - i_q$ components of \mathbf{q} . The vector $\mathbf{q}' = (q_{i_q+1}/S, \dots, q_m/S)$ is a probability distribution such that the ratio between its largest and its smallest component is upper bounded by 2. By Theorem 2, with $\rho = 2$, it follows that

$$H(\mathbf{q}') \geq \log(m - i_q) - \alpha, \quad (12)$$

where $\alpha \leq \left(1 - \frac{1 + \ln(\ln 2)}{\ln 2}\right) < 0.0861$. Therefore, we have

$$\begin{aligned} H(\mathbf{q}) &= \sum_{j=1}^{i_q} q_j \log \frac{1}{q_j} + \sum_{j=i_q+1}^m q_j \log \frac{1}{q_j} \\ &= \sum_{j=1}^{i_q} q_j \log \frac{1}{q_j} - S \log S + S \sum_{j=i_q+1}^m \frac{q_j}{S} \log \frac{S}{q_j} \end{aligned}$$

$$\begin{aligned}
&= \sum_{j=1}^{i_q} q_j \log \frac{1}{q_j} - S \log S + SH(\mathbf{q}') \\
&\geq \sum_{j=1}^{i_q} q_j \log \frac{1}{q_j} - S \log S + S(\log(m - i_q) - \alpha) \\
&= \sum_{j=1}^{i_q} q_j \log \frac{1}{q_j} + S \log \frac{m - i_q}{S} - \alpha S \\
&= \sum_{j=1}^{i_q} q_j \log \frac{1}{q_j} + \sum_{j=i_q+1}^m \frac{S}{m - i_q} \log \frac{m - i_q}{S} - \alpha S \\
&\geq \sum_{j=1}^{i_q} q_j \log \frac{1}{q_j} + \sum_{j=i_q+1}^m \frac{S}{m - i_q} \log \frac{m - i_q}{S} - \alpha \\
&= H\left(q_1, q_2, \dots, q_{i_q}, \frac{S}{m - i_q}, \dots, \frac{S}{m - i_q}\right) - \alpha.
\end{aligned}$$

Let $\mathbf{q}^* = (q_1, q_2, \dots, q_{i_q}, \frac{S}{m - i_q}, \frac{S}{m - i_q}, \dots, \frac{S}{m - i_q})$, and observe that \mathbf{q}^* coincides with \mathbf{p} in the first i_q components, as it does \mathbf{q} . What we have shown is that

$$H(\mathbf{q}) \geq H(\mathbf{q}^*) - \alpha. \quad (13)$$

We now observe that $i_q \leq i^*$, where i^* is the index that intervenes in the definition of our operator $R(\mathbf{p})$ (see (3)). In fact, by the definition of \mathbf{q} one has $q_{i_q} \geq q_{i_q+1} \geq \dots \geq q_m$, that also implies

$$\frac{\sum_{j=i_q+1}^m q_j}{m} \leq q_{i_q+1} \leq q_{i_q} = p_{i_q}. \quad (14)$$

Moreover, since the first i_q components of \mathbf{q} are the same as in \mathbf{p} , we also have $\sum_{j=i_q+1}^m q_j = \sum_{j=i_q+1}^n p_j$. This, together with relation (14), implies

$$\frac{\sum_{j=i_q+1}^n p_j}{m} \leq p_{i_q}. \quad (15)$$

Equation (15) clearly implies $i_q \leq i^*$ since i^* is by definition, the maximum index i such that $\sum_{j=i+1}^n p_j \geq (n - i)p_i$. From the just proved inequality $i^* \geq i_q$, we have also

$$\mathbf{q}^* \preceq R(\mathbf{p}). \quad (16)$$

Using (13), (16), and the Schur concavity of the entropy function, we get

$$H(\mathbf{q}) \geq H(\mathbf{q}^*) - \alpha \geq H(R(\mathbf{p})) - \alpha,$$

thus completing the proof of the Lemma (and of Theorem 1). \blacksquare

We now prove Theorem 2. Again, we use tools from majorization theory. Consider an arbitrary probability distribution $\mathbf{p} = (p_1, p_2, \dots, p_n)$ with $p_1 \geq p_2 \geq \dots \geq p_n > 0$ and $p_1/p_n \leq \rho$. Let us define the probability distribution

$$\begin{aligned}
\mathbf{z}_\rho(\mathbf{p}) &= (z_1, \dots, z_n) \\
&= (\underbrace{\rho p_n, \dots, \rho p_n}_{i \text{ times}}, 1 - (n + i\rho - i - 1)p_n, p_n, \dots, p_n),
\end{aligned} \quad (17)$$

where $i = \lfloor (1 - np_n)/p_n(\rho - 1) \rfloor$. It is easy to verify that $p_n \leq 1 - (n + i(\rho - 1) - 1)x \leq \rho p_n$.

Lemma 4. Let $\mathbf{p} = (p_1, p_2, \dots, p_n)$ with $p_1 \geq p_2 \geq \dots \geq p_n > 0$ be any probability distribution with $p_1/p_n \leq \rho$. The probability distribution $\mathbf{z}_\rho(\mathbf{p})$ satisfies $\mathbf{p} \preceq \mathbf{z}_\rho(\mathbf{p})$.

Proof: For any $j \leq i$, it holds that

$$p_1 + \dots + p_j \leq j p_1 \leq j(\rho p_n) = z_1 + \dots + z_j.$$

Consider now some $j \geq i + 1$ and assume by contradiction that $p_1 + \dots + p_j > z_1 + \dots + z_j$. It follows that $p_{j+1} + \dots + p_n < z_{j+1} + \dots + z_n = (n - j)p_n$. As a consequence we get the contradiction $p_n \leq (p_{j+1} + \dots + p_n)/(n - j) < p_n$. \blacksquare

Lemma 4 and the Schur concavity of the entropy imply that $H(\mathbf{p}) \geq H(\mathbf{z}_\rho(\mathbf{p}))$. We can therefore prove Theorem 2 by showing the appropriate upper bound on $\log n - H(\mathbf{z}_\rho(\mathbf{p}))$.

Lemma 5. It holds that

$$\log n - H(\mathbf{z}_\rho(\mathbf{p})) \leq \left(\frac{\rho \ln \rho}{\rho - 1} - 1 - \ln \frac{\rho \ln \rho}{\rho - 1} \right) \frac{1}{\ln 2}.$$

Proof: Consider the class of probability distributions of the form

$$\mathbf{z}_\rho(x, i) = (\rho x, \dots, \rho x, 1 - (n + i(\rho - 1) - 1)x, x, \dots, x),$$

having the first i components equal to ρx and the last $n - i - 1$ equal to x , for suitable $0 \leq x \leq 1/\rho$, and $i \geq 0$ such that

$$1 - (n + i(\rho - 1) - 1)x \in [x, \rho x]. \quad (18)$$

Clearly, for $x = p_n$ and $i = \lfloor (1 - np_n)/p_n(\rho - 1) \rfloor$ one has $\mathbf{z}_\rho(\mathbf{p}) = \mathbf{z}_\rho(x, i)$, and we can prove the lemma by upper bounding the maximum (over all x and i) of $\log n - H(\mathbf{z}_\rho(x, i))$. Let

$$\begin{aligned}
f(x, i) &= \log n - H(\mathbf{z}_\rho(x, i)) = \log n + i(\rho x \log(\rho x)) \\
&\quad + (1 - (n + i(\rho - 1) - 1)x) \log(1 - (n + i(\rho - 1) - 1)x) \\
&\quad + (n - i - 1)x \log x.
\end{aligned}$$

From (18), for any value of $i \in \{1, \dots, n - 2\}$, one has that

$$x \in \left(\frac{1}{n + (i + 1)(\rho - 1)}, \frac{1}{n + i(\rho - 1)} \right]$$

Set $A = n + i(\rho - 1) - 1$. We have

$$\begin{aligned}
f(x, i) &= \log n + i\rho x \log(\rho x) \\
&\quad - (1 - Ax) \log(1 - Ax) + (n - i - 1)x \log x,
\end{aligned}$$

$$\begin{aligned}
\frac{d}{dx} f(x, i) &= i\rho \log \rho + (i\rho - A + n - i - 1) \log e \\
&\quad + (i\rho + n - i - 1) \log x - A \log(1 - Ax) \\
&= i\rho \log \rho + A \log x - A \log(1 - Ax),
\end{aligned}$$

$$\frac{d^2}{dx^2} f(x, i) = \left(\frac{A}{x} + \frac{A^2}{1 - Ax} \right) \log e.$$

Since $\frac{d^2}{dx^2} f(x, i) \geq 0$ for any $x \in \left(\frac{1}{n + (i + 1)(\rho - 1)}, \frac{1}{n + i(\rho - 1)} \right]$, the function is \cup -convex in this interval, and it is upper bounded by the maximum between the two extrema values

$f(1/(n+(i+1)(\rho-1)), i)$ and $f(1/(n+i(\rho-1)), i)$. Therefore, we can upper bound $f(x, i)$ by the maximum value among

$$f(1/(n+i(\rho-1)), i) = \log n + \frac{i\rho}{n+i(\rho-1)} \log \rho + \log \frac{1}{n+i(\rho-1)},$$

for $i = 1, \dots, n-1$. We now interpret i as a continuous variable, and we differentiate $\log n + \frac{i\rho}{n+i(\rho-1)} \log \rho + \log \frac{1}{n+i(\rho-1)}$ with respect to i . We get

$$\begin{aligned} \frac{d}{di} \left(\log n + \frac{i\rho}{n+i(\rho-1)} \log \rho + \log \frac{1}{n+i(\rho-1)} \right) \\ = \frac{n(\rho \log \rho - (\rho-1) \log e) - i(\rho-1)^2 \log e}{(n+i(\rho-1))^2}, \end{aligned}$$

that is positive if and only if $i \leq \frac{n}{\rho-1} \left(\frac{\rho \ln \rho}{\rho-1} - 1 \right)$. Therefore, the desired upper bound on $f(x, i)$ can be obtained by computing the value of $f(\bar{x}, \bar{i})$, where $\bar{i} = \frac{n}{\rho-1} \left(\frac{\rho \ln \rho}{\rho-1} - 1 \right)$ and $\bar{x} = \frac{1}{n+\bar{i}(\rho-1)}$. The value of $f(\bar{x}, \bar{i})$ turns out to be equal to

$$\begin{aligned} \log n + \frac{\frac{n}{\rho-1} \left(\frac{\rho \ln \rho}{\rho-1} - 1 \right) \rho \log \rho}{n + n \left(\frac{\rho \ln \rho}{\rho-1} - 1 \right)} - \log \left(n + n \left(\frac{\rho \ln \rho}{\rho-1} - 1 \right) \right) \\ = \frac{\rho \log \rho (\rho \ln \rho - \rho + 1)}{(\rho-1) \rho \ln \rho} - \log \left(\frac{\rho \ln \rho}{\rho-1} \right) \\ = \frac{\rho \ln \rho - (\rho-1)}{(\rho-1) \ln 2} - \log \left(\frac{\rho \ln \rho}{\rho-1} \right) \\ = \left(\frac{\rho \ln \rho}{\rho-1} - 1 - \ln \frac{\rho \ln \rho}{\rho-1} \right) \frac{1}{\ln 2}. \end{aligned}$$

We conclude the paper by showing how Theorems 1 and 2 allow us to design an approximation algorithm for the second problem mentioned in Section III, that is, the problem of constructing a probability distribution $\bar{\mathbf{q}} = (\bar{q}_1, \dots, \bar{q}_m)$ such that $D(\mathbf{p}, \bar{\mathbf{q}}) \leq D(\mathbf{p}, \mathbf{q}^*) + 0.0861$. Our algorithm improves on the result presented in [4], where an approximation algorithm for the same problem with an additive error of 1 was provided.

Let \mathbf{q} be the probability distribution constructed in Lemma 3 and let us recall that the first i_q components of \mathbf{q} coincide with the first i_q components of \mathbf{p} . In addition, for each $i = i_q + 1, \dots, m$, there is a set $I_i \subseteq \{i_q + 1, \dots, n\}$ such that $q_i = \sum_{k \in I_i} p_k$ and the I_i 's form a partition of $\{i_q + 1, \dots, n\}$, (i.e., \mathbf{q} is an aggregation of \mathbf{p} into m components).

We now build a bivariate probability distribution $\mathbf{M}_q = [m_{ij}]$, having \mathbf{p} and \mathbf{q} as marginals, as follows:

- in the first i_q rows and columns, the matrix \mathbf{M}_q has non-zero components only on the diagonal, namely $m_{ij} = p_j = q_j$ and $m_{ij} = 0$ for any $i, j \leq i_q$ such that $i \neq j$;
- for each row $i = i_q + 1, \dots, m$ the only non-zero elements are the ones in the columns corresponding to elements of I_i and precisely, for each $j \in I_i$ we set $m_{ij} = p_j$.

It is not hard to see that \mathbf{M}_q has \mathbf{p} and \mathbf{q} as marginals. Moreover we have that $H(\mathbf{M}_q) = H(\mathbf{p})$ since by construction

the only non-zero components of \mathbf{M}_q coincide with the set of components of \mathbf{p} . Let $\mathcal{C}(\mathbf{p}, \mathbf{q})$ be the set of all bivariate probability distribution having \mathbf{p} and \mathbf{q} as marginals. Recall that $\alpha = 1 - (1 + \ln(\ln 2))/\ln 2 < 0.0861$. We have that

$$D(\mathbf{p}, \mathbf{q}) = \min_{\mathbf{N} \in \mathcal{C}(\mathbf{p}, \mathbf{q})} 2H(\mathbf{N}) - H(\mathbf{p}) - H(\mathbf{q}) \quad (19)$$

$$\leq 2H(\mathbf{M}_q) - H(\mathbf{p}) - H(\mathbf{q}) \quad (20)$$

$$= H(\mathbf{p}) - H(\mathbf{q}) \quad (21)$$

$$\leq H(\mathbf{p}) - H(R_m(\mathbf{p})) + \alpha \quad (22)$$

$$\leq H(\mathbf{p}) - H(\mathbf{q}^*) + \alpha \quad (23)$$

$$\leq D(\mathbf{p}, \mathbf{q}^*) + \alpha \quad (24)$$

where (19) is the definition of $D(\mathbf{p}, \mathbf{q})$; (20) follows from (19) since $\mathbf{M}_q \in \mathcal{C}(\mathbf{p}, \mathbf{q})$; (21) follows from (20) because of $H(\mathbf{M}) = H(\mathbf{p})$; (22) follows from Lemma 3; (23) follows from (22), the known fact that \mathbf{q}^* is an aggregation of \mathbf{p} (see [18]) and Lemmas 1 and 2. Finally, the general inequality $H(\mathbf{a}) - H(\mathbf{b}) \leq D(\mathbf{a}, \mathbf{b})$ is formula (48) in [12].

REFERENCES

- [1] J.C. Baez, T. Fritz and T. Leinster, "A Characterization of entropy in terms of information loss", *Entropy*, vol. **17**, 772–789, 2015.
- [2] F. Cicalese and U. Vaccaro, "Supermodularity and subadditivity properties of the entropy on the majorization lattice", *IEEE Transactions on Information Theory*, vol. **48**, 933–938, 2002.
- [3] F. Cicalese and U. Vaccaro, "Bounding the average length of optimal source codes via majorization theory", *IEEE Transactions on Information Theory*, vol. **50**, 633–637, 2004.
- [4] F. Cicalese, L. Gargano, and U. Vaccaro, "Approximating probability distributions with short vectors, via information theoretic distance measures", in: *Proceedings of ISIT 2016*, pp. 1138–1142, 2016.
- [5] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley-Interscience; 2nd edition (2006).
- [6] L. Faivishevsky and J. Faivishevsky, "Nonparametric information theoretic clustering algorithm", in: *Proceedings of the 27th International Conference on Machine Learning (ICML-10)*, pp. 351–358, 2010.
- [7] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness*, W. H. Freeman (1979).
- [8] B.C. Geiger and R.A. Amjad, "Hard Clusters Maximize Mutual Information", arXiv:1608.04872 [cs.IT]
- [9] S.W. Ho and R.W. Yeung, "The interplay between entropy and variational distance", *IEEE Trans. Inf. Theory*, **56**, 5906–5929, 2010.
- [10] S. W. Ho and S. Verdù, "On the interplay between conditional entropy and error probability", *IEEE Trans. Inf. Theory*, **56**, 5930–5942, 2010.
- [11] M. Kearns, Y. Mansour, and A. Y. Ng, "An information-theoretic analysis of hard and soft assignment methods for clustering." In: *Learning in graphical models*. Springer Netherlands, pp. 495–520, 1998.
- [12] M. Kovačević, I. Stanojević, and V. Senk, "On the Entropy of Couplings", *Information and Computation*, Vol. **242**, (2015). 369–382.
- [13] B.M. Kurkoski, and H. Yagi, "Quantization of binary-input discrete memoryless channels", *IEEE Transactions Information Theory*, vol. **60**, 4544 – 4552, 2014.
- [14] P. Malacaria and J. Heusser, "Information theory and security: Quantitative information flow", in: Aldini A. et al. (eds) *Formal Methods for Quantitative Aspects of Programming Languages. SFM 2010*. Lecture Notes in Computer Science, vol. **6154**. Springer, Berlin, Heidelberg.
- [15] A.W. Marshall, I. Olkin, B. C. Arnold, *Inequalities: Theory of Majorization and Its Applications*, Springer, New York (2009).
- [16] D. Muresan and M. Effros, "Quantization as histogram segmentation: Optimal scalar quantizer design in network systems", *IEEE Transactions on Information Theory*, vol. **54**, 344–366 (2008).
- [17] S. Simic, "Jensen's inequality and new entropy bounds." *Appl. Math. Letters*, **22**, 1262–1265, 2009.
- [18] M. Vidyasagar, "A metric between probability distributions on finite sets of different cardinalities and applications to order reduction", *IEEE Transactions on Automatic Control*, vol. **57**, 2464–2477, 2012.